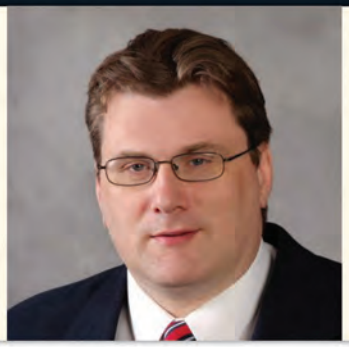
VIEWS & VISIONS

A publication of Bowles Rice LLP

Summer 2015



Social Engineering and the Modern "Hacker"

Bill Gardner, Assistant Professor, Marshall University
Evan R. Kime, Partner, Bowles Rice LLP

Bill Gardner is an Assistant Professor at Marshall University, where he teaches in the Digital Forensic and Information Assurance Program. He is also President and Principal Security Consultant at BlackRock Consulting and the Information Security Chair at the Appalachian Institute of Digital Evidence.

Prior to joining the faculty at Marshall, Bill co-founded the 304Geeks and Hack3rCon. He is the coauthor of "*Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*" with Valerie Thomas, and a co-author of the latest revision of "*Google Hacking for Penetration Testers*," which will be out this summer.

Evan R. Kime is a partner in the Charleston, West Virginia office of Bowles Rice. He concentrates his practice in business litigation, including insurance "bad faith" defense, mass and toxic torts, and employer's liability.

Before pursuing his law degree from West Virginia University College of Law, Evan worked as a systems engineer for Lockheed Martin at the Criminal Justice Information Systems Center in Clarksburg, West Virginia and the West Virginia State Police Headquarters in South Charleston, West Virginia, where he administered the Automated Fingerprint Identification System for state and federal authorities.

When we speak of hackers, most people see an image of a hoodie-wearing whiz-kid, feverishly banging away at the keyboard, launching a technical onslaught that somehow slips in behind an organization's firewall. That image is mostly mythology.

Typically, today's attackers are not exploiting a glitch in your system's code or opening ports in your firewall. Instead, they are coming through your organization's firewall and other defenses disguised as normal, innocuous data traffic, by exploiting the weakest link in your defenses: your people. Using a tactic called "social engineering," hackers (or "social engineers") prey upon your people's natural inclination to be helpful. Social engineering has been defined as the clever manipulation of the natural human tendency to trust. In data security, people are always the weakest link because they want to be helpful. They want to provide good customer service, they want to be polite, and they are too easily tricked.

It is likely that your company's personnel have developed some unfortunate online habits that are based on misplaced trust and naiveté when it comes to technology. These habits can be hard to break. For example, if an attachment or link "looks like" it's from one of your clients, most employees are going to open the attachment because they want to be helpful to the client and do a good job. So, from the hacker's perspective, why bother trying to pick the lock on the firewall when an insider will hold the door open for you?

Here are some examples of how social engineering works.

The most common form of social engineering attacks involve "phishing." Phishing attacks are emails that attempt to entice the receiver into clicking a link in the body of an email or opening an attachment. Once a user on the inside clicks the fake link, the user's computer becomes infected with malicious software ("malware") that installs itself and runs in the background. A phishing attack may also involve a fake website that is nearly identical to a legitimate one, designed to collect financial or personal information.

Another common attack involves a hyperlink that allows the hacker access to the victim's computer using "exploit software." This type of

attack completely bypasses all the technical defenses on the victim's network and, once inside, the hacker frequently uses a method called "pivoting" to attack other systems on the same network.

Social engineering attacks can also arrive in person. Someone poses as a legitimate visitor like a vendor or delivery person and physically gains access to your office or building. Once inside, the attacker can place rogue wireless access points, or even steal computers that contain confidential data.

Social engineering is not new. In fact, hackers have used it for many years. Take renowned hacker Kevin Mitnick, for example. In 1999, Mitnick was convicted of a number of serious computer and communications-related crimes wherein he accessed the systems of several high-profile targets, just by asking the right people to volunteer the right sensitive information. Mitnick's hacking exploits earned him a spot on the FBI's Most Wanted list. Even so, before he was apprehended he dodged authorities by hacking the voicemail of the FBI agents pursuing him!

Cyber crime such as hacking is a multi-billion dollar a year industry, and organized crime has become heavily involved. The motives vary. Most attackers are looking for data they can sell for money. Moreover, the information security threat is global. The Russian Business Network is an organized computer-crime syndicate that targets your personal identity information, such as Social Security numbers and medical records, and sells them on the black market. Hackers from China, on the other hand, are usually after intellectual property or trade secrets that can be sold to competitors or used to gain a competitive edge. "Hacktivists," such as the group known as "Anonymous," are also global, and use social engineering for political means, breaking into networks of organizations that represent a contrary world view, defacing websites and disseminating sensitive information.

The best defense against social engineering attacks is awareness and education. If your employees understand what might happen when they click on links or open attachments from unknown sources, they are more likely to recognize and report questionable emails, attachments and internet links. The first step is to get your employees to understand that your company's data is valuable to hackers who wish to steal it and sell it. Employees must recognize that there are huge risks at stake for the company, and they are the first line of defense.

Second, it is imperative that employees are educated about what they can do to prevent social engineers from taking advantage of them. These measures can be as simple as holding yearly training or making information security awareness, including the threats of social engineering, a part of the on-boarding process. Using recent, well-publicized news stories about cyber attacks and data breaches that have happened to other businesses and organizations will help illustrate the threat to your employees.

In the final analysis, the threat of "hacking" may not lie where you think. Social engineers do not have to be computer geniuses to make trouble. However, proper education and a healthy dose of caution will ensure that risks to your organization are minimized.